An Efficient Ensemble Architecture for Privacy and Security of Electronic Medical Records

Ömer Kasım
Department of Electrical and Electronics Engineering
Kutahya Dumlupinar University, Turkey
omer.kasim@dpu.edu.tr

Abstract: *Electronic medical records, one of the sensitive data, are stored in public or private cloud service providers. Cloud systems provide security with firewall and intrusion detection systems, and these systems ensure privacy with access control and end-to-end encryption. However, while sending data to the cloud system, attackers can capture the data with the help of Man in the Middle attacks and vulnerabilities of the storage systems. In the middleware architecture proposed in this study, access control protocol, key distributor and end-to-end hybrid encryption which are based on user roles were innovatively used to overcome security issues in data transmission. In this system, writing and updating requests are encrypted asymmetrically, and reading requests were encrypted symmetrically. This solution distinguishes the proposed method from previous studies. According to this solution the operating performance of the system is increased. In addition, the attacker cannot see the actual data in a cyber-attacks because the sensitive data is distributed to the users with their private keys. This result shows that the access, write and update of electronic medical records are performed with the principles of security and privacy.*

Keywords: *Electronic medical records, sensitive data security, hybrid encryption and decryption, access control.*

Received December 15, 2020; accepted August 17, 2021
https://doi.org/10.34028/iajit/19/2/14

1. Introduction

Nowadays, there is a huge increase in the amount of data that produced and used [16]. Some of the produced data can be seen by everyone as public data according to the user's decision [24]. However, personal data should be kept securely. It is also important to control access without violating the confidentiality of these type of data [12, 15]. One of the sensitive data is Electronic Medical Records (EMR) [11]. When the person takes the healthcare, various examinations are made while using the health service. These examinations are evaluated by experts. Using these evaluations, the expert applies the diagnosis and treatment processes to the person. All data obtained in this process are stored as EMR. These EMRs are stored in the data centers of the hospitals and in the cloud. Generally, EMRs in the cloud environment are stored in a private cloud [31].

Access and use of EMRs are important for the security and confidentiality of personal sensitive data. Firstly, user authorization is performed to achieve them [48]. Then, the security process is managed with firewall systems, logging and Intrusion Detection System (IDS) systems [10]. Quite strict security rules are used in accessing the EMRs. Despite these rules, many of the recent cyber-attacks were performed to health institutions [2, 27]. In these attacks, Denial of Service (Dos), Distributed Denial of Service (DDos), Structured Query Language (SQL) injection, Cross Site Scripting (XSS) code attacks and Man in the Middle (MIM) attacks methods were used by the attackers to obtain the EMRs [50].

When patients' exponentially growing medical records are stored in the cloud, the data stream needs to be encrypted. However, recent decryption activities of attackers, such as quantum cryptography, require more efficient encryption. In the method developed in this study, access to EMRs is determined by the roles of the authorized users according to the eXtensible Access Control Markup Language (XACML) standard. Authorization is performed in the roles of patient, medical staff and researchers. The patient user can only see EMRs. The medical staff has the authority to read, update and add EMRs. The researcher has the role of only reading the data in the specified tables in the database. It is especially important to encrypt the data when transferring the data to a different IP [40]. The transactions that users will perform according to their roles are encrypted with Advanced Encryption Standard (AES) and RSA [39]. The easy implementation of AES and Rivest-Shamir-Adleman encryption (RSA) is the motivation of the study. The query contents of the medical staff user role are encrypted with AES. These data are written and updated to the database as AES encrypted. In reading query, AES is decrypted and the requested data is displayed to the medical staff user role. In patient and researcher user roles EMRs are encrypted with RSA and signed with a private key. Then, the signed data transmitted to the user. The user who has a signature

key can decrypt the signed EMR with the private key and the public key. Public and private keys are distributed to users with the key distributor system developed innovatively in the study The main contributions of this study are as follows.

1. Since the hybrid use of AES and RSA requires the attacker to find the private key and the public key, in MIM attacks the attacker only sees the encrypted data. This ensures the privacy and security of EMRs.
2. In the experiments, AES decryption time was calculated as 2.14 seconds and RSA decryption time was calculated as 10.52 seconds. This result adds to the performance of the system compared to asymmetric encryption performance.
3. The comprehensive experiment was conducted using the middleware based hybrid encryption and key distributer to verify the effectiveness of the proposed approach.

The article is organized as follows. Section 2 covers the related works. Section 3 discusses the proposed approach based on middleware system analysis. Simulation results are given in section 4. Finally, the brief discussion of this study is given in section 5.

2. Related Work

When the sharing of data related to EMRs increases, it must be stored in the cloud environment. Solutions for security and privacy are offered in the cloud environment. However, the data transferred to the cloud environment with different attack techniques can be obtained by the attackers. It is recommended in the literature to encrypt EMRs locally before sending them to cloud providers. In this respect, encryption with different encryption algorithms is widely used [26].

Various studies have been proposed in the literature for the safety of medical data. Symmetrical and asymmetrical encryption methods were used in these studies. These methods have different advantages and disadvantages. The results obtained in various studies are given below.

Yilmaz and Tarhan [49] proposed a 2-dimensional evaluation method that includes code and operation that users take to measure security. The attributes of the access records in the database of open source systems are examined in this method. As a result of the examination, security operations are carried out. Tuncer and Avci [44] used a cryptologic approach for data security in their study. In this approach, data is encrypted according to the characters of Gokturk alphabet and data security is ensured. Liu *et al*. [23] Ciphertext-Policy Attribute-Based Encryption (CP-ABE) provides fine-grained access control of encrypted data in the cloud.

Unlike cryptology approaches, access control applications are included in the literature. In these applications, Mandatory Access Control (MAC) and Role-Based Access Control (RBAC) models are used [36]. Soni and Kumar [43] proposed privacy-sensitive access control rules on systems using MAC and RBAC. They proposed a framework that supports the management of these rules. In another study, the Usage Control (UCON) model created according to the Digital Rights Management (DRM) requirements was used [37]. It includes a Conceptual Framework (CF) that includes model access control. Therefore, contribution has been made to ensuring usage control. Yang *et al*. [47] used the Platform for Privacy Preferences (P3P), which is a standardized privacy preference policy by the World Wide Web Consortium (W3C). P3P provides privacy applications to be automatically received by user agents. Another platform is Enterprise Privacy Authorization Language (EPAL). Data usage purposes are specified for users with certain roles in certain conditions that may occur in EPAL. A Logic Program (LP) model is used to specify these objectives [41].

XACML is used to provide rules independent of applications [7]. A Role-Based Access Control model (RBAC) to apply privacy policies to the hybrid system that formed in his study [1]. Dinur *et al*. [6] and Kleinberg *et al*. [20] used statistics-based query answering system in their study. In these studies, which are based on interactive statistical approach, access to the entire dataset of queries generated by the user is prevented. Only batch queries sent by the user are responded. Kenthapadi *et al*. [17] used query control to ensure that the user who received the data could not obtain sensitive information. Access to the sensitive data is denied with this control. Dwork *et al*. [9] used the Output Deviation Technique (ODT) to give an uneasy answer to the data recipient. In these studies, the data collector is allowed to publish the data records instead of publishing the query results. Since these methods can have a lot of clear and historical information, they have a strong guarantee of the limited attack model that is open to a practical solution [8, 18, 35, 49].

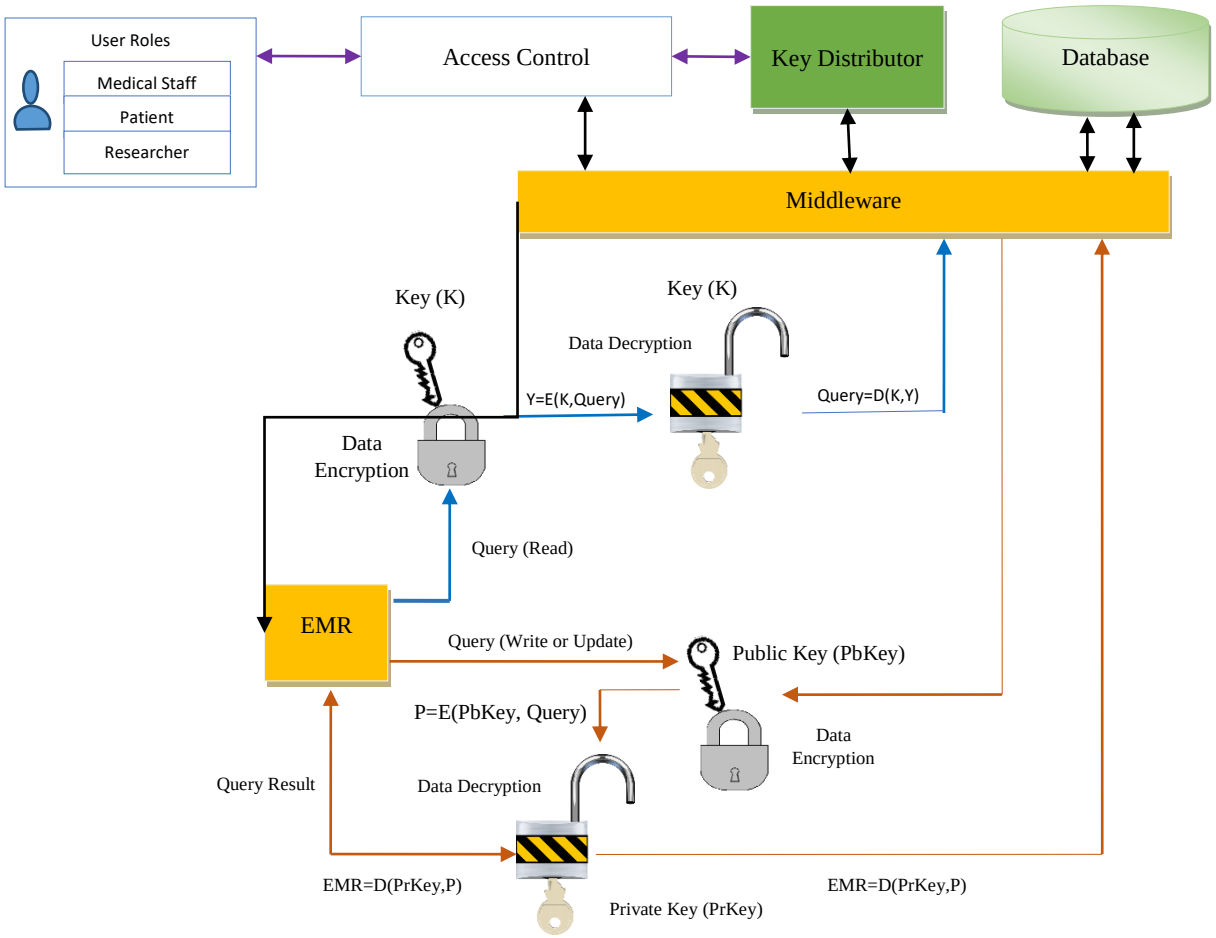

Figure 1. The schema of the proposed method.

In hybrid approaches suggested in the literature, Mukti and Setiawan [28] showed in their study that AES and RSA can be used in EMR encryption. While using AES for encryption, the authors assigned an RSA Digital Signature to the data encrypted via the web application. They provided a unique end-to-end encryption for each healthcare staff who was given a private key with the user role with this signature. Khozaimi *et al*. [19] applied AES encryption to EMRs in their study. Unique key provided with Fingerprint. The authors stated that they found more successful results in terms of performance when they compared encryption with algorithms such as RSA and DES. Osamor and Edosomwan [29] proposed a different approach to increase the encryption difficulty of the RSA encryption algorithm. The authors obtained the difficulty of decryption factor by changing the private key sequence with the scrambled alpha-numeric randomization technique. In addition, it was stated that hybrid solutions where RSA and AES are used together can be more effective [5].

In addition to them, query analysis and key search are also used for security in the transmission of medical data. In Secure Multi-Party Computation (SMC), a subcategory of cryptology, and queries with special inputs are used to ensure confidentiality. Oblivious Transfer (OT) [30], Homomorphic Encryption (HE) [13] and Oblivious Polynomial Evaluation (OPE) [46] are used in the literature. Another option is based on performing this control over the protocol. Private Information Retrieval (PIR), which is a special information retrieval protocol, provides access to data by sending a query to a server that has a database without revealing the item that the user receives the query result [36]. The Single Keyword Search (SKS) [42] and the Conjunctive Keyword Search (CKS) [3] methods, which use symmetric encryption, are used to send queries for encrypted data. These methods provide a safe search for the user with the keyword in the query to get the relevant documents. In the Attribute Based Encryption (ABE) method [22], users' keys and encrypted data are tagged with descriptive attributes. The data is decrypted if the key of the user who receives the data received as a result of a specific key in the labeling matches the key. Key Policy Attribute Based Encryption (KP-ABE) [22] and Encrypted Text Attribute Based Encryption (ET-ABE) are two methods used for access control [45]. Although these methods provide a guarantee of privacy protection, they are often impractical due to performance constraints and high costs.

Although studies such as key distribution, matching of the keyword in the query, using AES and RSA together are suggested in the literature, it is suggested in this study to give a private key or to regulate

encryption with access to certain tables when necessary based on the role. This makes it incompetent for attackers to decrypt with AES or RSA, but also requires them to know what role the person in charge is doing the encryption. HE is unnecessary in key distribution, and time is not wasted with key matching with the role-based encryption. In addition, the disadvantages of symmetric and asymmetric encryption relative to each other cannot be eliminated.

3. Proposed Hybrid Encryption Model

AES was used as symmetric encryption in the proposed method. AES is particularly resistant to decryption algorithms in quantum cryptography [21]. In AES, the key must be transmitted securely between the sender and the receiver [47]. The encrypted chipper text obtained with 10 rounds is obtained with a public key. This disadvantage disappears when the RSA algorithm, which is especially vulnerable to decryption algorithms, is used with AES [5]. In RSA, different keys are used for encryption and decryption processes. One of these keys is the public key. The public key is public and distributed to system users. The other key is the secret key. The private key is given to each user individually

As the speed of access to the data is high, AES was preferred for encryption with public key. EMRs created by users with the role of medical staff users are taken from the fields in the interface with 256 bit AES, encrypted in middleware and transferred to the database. Users in the role of medical staff view this data in the system interface using select queries. Users other than the medical staff role can only access the data. In the access process, the data are signed with the private key in the middleware system and sent to the user. RSA algorithm was used for signing with private key because of the secure signing it provides. When encrypted data created with public key and private key are obtained with the MIM attack, the data is secured as attackers will only see a single hex content. Users can see the data by verifying signature with their private key. The block diagram of the proposed method is shown in Figure 1. EMRs are stored in 7 tables in the database. Information in the categories of medical history, physical examination, medical record, laboratory tests, family data, community data, consultants and medical history are included in the EMRs. These data stored in the database are kept in various tables according to the design. Database design is shown in Figure 2.

In the proposed model, the query can be designed to read data, write data or update data. When users with different roles create a reading query from these three types of queries, the query is encrypted with symmetric encryption using Y=E (K, Query). The RSA algorithm using the same public key is used in the AES and private key (W). The purpose of the query request design is to ensure that users with the common key can submit queries. Users without the key will not be able to access the database because they are not defined. It is provided with the access control system with XACML standard for key distribution. In this standard, 4 different situations are applied to the user request code. These are permit, deny, indeterminate and not applicable.

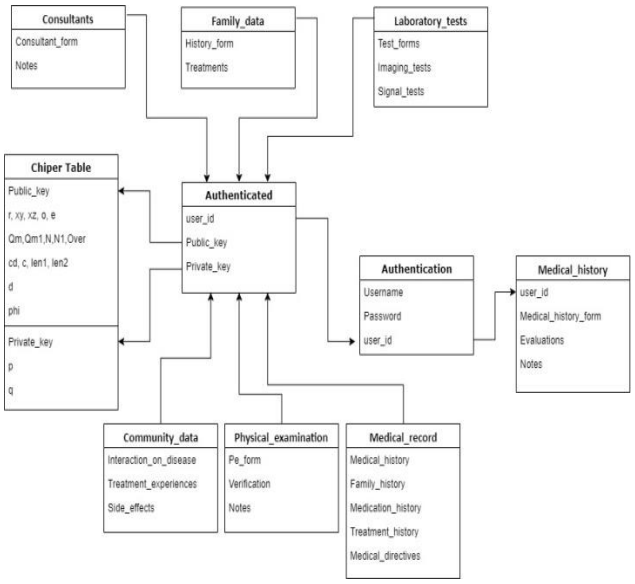

Figure 2. EMR Database UML diagram.

After access control, users who are included in the system and have a symmetric password key send their reading queries to the middleware software with RSA. Middleware software resolves incoming query requests with Query=D (K, Y) and encrypts EMRs from the database with AES. Data encrypted with P=E (PbKey, Query) is returned to the user using the Public Key (PbKey) and private key (PrKey) and RSA encryption algorithm. The data received by the user is analyzed with EMR=D (PrKey, P) used in asymmetric encryption.

4. Experimental Results

In the architecture developed in this study, registered users have the roles of patients, medical staff or researchers. Each user's own private key and the system's public key are delivered to the middleware system and access control module by the key distributor module. When the user name, user role and keys match, the user logs into the system with the XACML standard in the control module. Only the medical staff user from the logged in users has the ability to write data and send data by update queries. Other users' interfaces only have operations for reading queries. Since data writing and data update queries which contain EMR, the query request is encrypted with symmetric encryption containing public key. When the request for reading is sent according to the user role of the logged in, symmetric encryption

process containing the AES algorithm is applied to the query. In symmetric encryption, key pairs are used as modulus 5723, Public Exponent 5 and private exponent 3341.

The encryption cipher text occurs when the "update Medical-history set Evaluations='Cancer' where user-id=123", which is the query to see the users with the user request reading EMR, is encrypted. The content in the read query request is difficult for attackers who do not know the key pairs. When the reading query reaches the middleware software, decryption is performed. Decryption is created with signature key pair. If parsing is done with the key pair, the signature is verified. When is Verified is Ok, query request is resolved and it is obtained as a Restored Message. A time of 0.009 sec is spent for reading a 10-byte data from database table. The time taken to read the entire EMR of 5784 bytes was measured as 16.35 seconds.

Asymmetric encryption was used in the study while middleware system read the data from the database and delivered it to the user in line with the queries it solved. In asymmetric encryption and decryption scheme, prime number for public key (p) and private key (q) is taken from key distributor. A medical staff user took p=11 and q=17 in experiment. Then, n=187 phi=160 and d=37 were calculated. As a result of the RSA algorithm, Public Key 13,187 and private key 37,187 were obtained. The update query encrypted with public and private key is asymmetrically encrypted. 0.022 sec is spent in the query made to see data in only one field. Since the private key is private to each user, data is encrypted according to the user signature. The time taken to read the entire EMR of 5784 bytes was measured as 10.52 seconds.

In the hybrid encryption process, the EMR in variable Nm1 is written to the database encrypted in the process of writing data to the database. The data converted as M1 as a result of writing is stored in the database as obtained in step c1. The parameters used to encrypt the data are determined according to the key generated by the key generator. These key values are assigned to the user as private (p, q) and public (d, r, xy, xz, phi, qmqm1, c, over, o, nm, n1, n, m, len1len, e and diff). Depending on these key values, access is decoded with decryption in access control. Users and attackers who do not have these keys see the result in step c1 when they receive the data.

5. Discussions

In this study, the access process to the database running on the private cloud is encrypted. The access controller determines the types of queries that can be made according to the type of user logged in. While the patient user can only read data, the researcher user has the roles of reading the data allowed by the patient user, and the health worker has the roles of reading and writing. EMRs are delivered to the end user according to the right of access. In various studies conducted in the literature, privacy and security are provided by different methods (Table 1). The method developed in this study is provided with the access method including the privacy XACML standard and key distributer. The key distributer contains a private key for each user and the public key of the system. The fact that users who are not defined in the system do not have a key prevents access to the system. The security of the data is provided by hybrid encryption.

Table 1. Privacy and security solutions.

Literature Studies	Privacy	Security
Yilmaz and Tarhan [49]	-	Attributes based logs
Tuncer and Avci [44]	-	Encryption with Gokturk alphabet
Soni and Kumar [43]	MAC, RBAC	on framework
Shaqrah and Noor [37]	UCO	CF
Yang *et al*. [47]	P3P	-
Singh *et al*. [41]	EPAL	-
Dinur *et al*. [6] Kleinberg *et al*. [20]	Query analysis	Allow or block
Kenthapadi *et al*. [17]	Query analysis	Allow or block
Dwork *et al*. [9]	Query analysis	ODT
OT [30], HE [13], OPE [46]	SMC	private information
PIR [36]	Chipper database	Query analysis
SKS [42], CKS [3]	Symmetric Encryption	Query analysis
ABE [22], KP-ABE [22], ET-ABE [45]	labeling with attributes	Key matching
Mukti and Setiawan [28]	Digital Signiture	Hybrid with AES and RSA
Khozaimi *et al*. [19]	Unique key	AES
Osamor and Edosomwan [29]	alpha-numeric randomization	RSA
Proposed Method	2 side key authentication	Hybrid with AES and RSA

Encrypting data with a user-specific key in asymmetric encryption is safer than DES and AES encryption methods. However, as shown in Table 2, the RSA algorithm does not offer a security solution against various attacks. The solution of this problem was overcome with hybrid encryption and 2 side key authentication performed in the study. In literature various effective algorithm is used for encryption of data. These are key distributer as Diffie-Hellman and Elliptic Curve Cryptography (ECC) algorithms. Although the ECC and more encrypted bits algorithm have explicit advantage, all of the cryptologic algorithms can be cracked in a manner ways. Thus AES 128 bit and RSA hybrid solution can provide very fast and simple encryption and verification. Also it is easier to implement and easier to understand than ECC. Therefore access control, key distribution and hybrid encryption and decryption is used in proposed method as middleware design.

Table 2. Comparison of security features [25].

Functionality	DES	AES	RSA
Privileged insider attack	Yes	No	No
Man-in-the-middle attack	No	No	No
Online password guessing attack	Yes	Yes	No
Flexible Access Control	No	No	No
Multiple Domain Access	No	No	No

In similar hybrid studies, data security was ensured only with digital signature related to medical staff. Other user roles are not included in the study [28]. In another study, AES encryption was performed with only a unique key [19]. The authors stated that they preferred AES to get better performance than DES and RSA. Compared to the method proposed in this study, the personalized key is not generated in the study. In another study, which aimed to further strengthen RSA, a stronger encryption was proposed [29]. However, RSA is slower than AES in terms of performance. The inclusion of AES in encryption for performance increase offers advantages in terms of encryption and decryption time [5].

The users entering the system according to their roles are symmetrically encrypted with the EMR system and the reading query requests received from the access controller. These requests reach the middleware system in front of the database. The read query requests are sent to the database and medical data are taken. Middleware system encrypts the query result with RSA algorithm by using private key and public key. Data which is asymmetrically encrypted is sent to the user. In addition, since writing requests contain medical data, they are encrypted asymmetrically and sent to the middleware request. Security is provided in transferring data from end to end with the hybrid encryption method using both symmetric and asymmetric encryption used in this study. Even if the MIM attack or a host is captured and the data is read, the private key is unique to each user, so the data becomes very difficult to decipher. Even if symmetric encryption is used, the system can work fast but the data can be analyzed because the public key is common. Asymmetric encryption is a disadvantage due to its slow operation. The hybrid encryption method works faster than the methods used asymmetric encryption. This improves the operating performance of the system. Features query requests were sent very quickly, and performance was increased.

Performance metrics obtained in the studies conducted in the literature are given in Figure 3. AES has the fastest performance and RSA has the slowest performance in the performance of the AES, RSA and DES encryption algorithms used for encrypting data [4]. In encryption systems made with a hardware solution instead of software, the system developed by Chua has obtained 2, 372s and other methods have obtained chipper text as 0.141, 0.162 and 1.03. In the performance measurements of the system developed in study, the system spent 20% performance in symmetric encryption and 80% CPU cost in asymmetric encryption. 0.112 seconds in AES encryption of an EMB of 1KB with these metrics. It was determined that it spent 3, 226 seconds in hybrid encryption. When evaluated as general performance, the system spends an average of 2, 101s per update request [14].

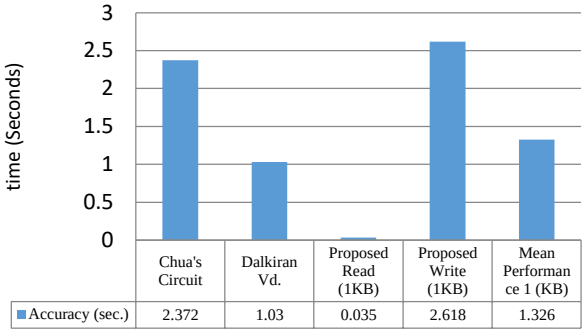

Figure 3. Performance Metrics of the proposed method.

Encryption and decryption processes are performed in the middleware system that is located between the access control and the database. The database is designed on the system developed as a private cloud. Requests received through the private cloud are answered if a role is assigned to the user. Otherwise, the request is thrown away in middleware. AES algorithm is used because it has higher features in terms of speed and performance in the transfer of data. AES algorithm provides efficiency in terms of system performance since it operates more optimized than other algorithms [33, 38]. RSA is used in many systems as an encryption algorithm that offers private key feature [35]. Although RSA is a known method, a password that becomes very difficult to decipher with the private key and public key produced by the key generator emerges in hybrid encryption. Since the keys are almost impossible to decipher without knowing the keys, security and privacy are provided in EMRs. Based on electronic health record system data sharing, threshold encryption technology, the proposed system can only be accessed when there are a threshold number of authorized users [34]. This scenario has been made more practical with the middleware system. On another method, patients and health institutions are recorded in encrypted form of health and medical prescription data. For encryption, double encryption technique with password text ID known as classes is used to increase security. The key owner includes a master secret key used to extract secret keys for various classes. The extracted key accumulates and transmits it to the patient as a single batch key for decryption purposes [32]. In the proposed study, anonymity and secure authentication of the users can be ensured.

6. Conclusions

When patients' exponentially growing medical records are stored in the cloud, the data stream needs to be encrypted. Data integrity and security of EMRs was ensured with hybrid encryption and access control used in this study. Asymmetric encryption time is longer than symmetric encryption. Using a user-specific key in data writing and updating ensures data security end to end. The performance of the system was increased by 10% by encrypting the queries with AES in terms of data access. This result has contributed to more secure EMRs and faster access speed than asymmetric encryption methods. Analysis and test results show that our system meets three important features: protocol security, transaction confidentiality and identity traceability. In future works, the constraints of the AES and RSA can be compensated by combining it with algorithms such as elliptic curve cryptology with better encryption.

References

[1] Ammar N., Malik Z., Bertino E., and Rezgui A., "XACML Policy Evaluation with Dynamic Context Handling," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 9, pp. 2575-2588, 2015.

[2] Balamurugan V. and Saravanan R., "Enhanced Intrusion Detection and Prevention System on Cloud Environment Using Hybrid Classification and OTS Generation," *Cluster Computing*, vol. 22, no. 3, pp. 13027-13039, 2019.

[3] Ballard L., Kamara S., and Monrose F., "Achieving Efficient Conjunctive Keyword Searches Over Encrypted Data," *in Proceedings of International Conference on Information and Communications Security*, Beijing, pp. 414-426, 2005.

[4] Dalkiran I. and Danişman K., "Artificial Neural Network Based Chaotic Generator for Cryptology," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 18, no. 2, pp. 225-240, 2010.

[5] Denis R. and Madhubala P., "Hybrid Data Encryption Model Integrating Multi-Objective Adaptive Genetic Algorithm for Secure Medical Data Communication Over Cloud-Based Healthcare Systems," *Multimedia Tools and Applications*, vol. 80, no. 11, pp. 21165-21202, 2021.

[6] Dinur I., Keller N., and Klein O., "An Optimal Distributed Discrete Log Protocol with Applications to Homomorphic Secret Sharing," *in Proceedings of 38th International Cryptology Conference*, Santa Barbara, pp. 213-242, 2018.

[7] Drozdowicz M., Ganzha M., and Paprzycki M., "Semantically Enriched Data Access Policies in Ehealth," *Journal of Medical Systems*, vol. 40, no. 11, pp. 1-8, 2016.

[8] Dwork C., "Differential Privacy: A Survey of Results," *in Proceedings of International Conference on Theory and Applications of Models of Computation*, Xi'an, pp. 1-19, 2008.

[9] Dwork C., McSherry F., Nissim K., and Smith A., "Calibrating Noise to Sensitivity in Private Data Analysis," *in Proceedings of Theory of Cryptography Conference*, New York, pp. 265-284, 2006.

[10] Elhoseny M., Ramírez-González G., Abu-Elnasr O., Shawkat S., Arunkumar N., and Farouk A., "Secure Medical Data Transmission Model for Iot-Based Healthcare Systems," *IEEE Access*, vol. 6, pp. 20596-20608, 2018.

[11] Fan K., Wang S., Ren Y., Li H., and Yang Y., "Medblock: Efficient and Secure Medical Data Sharing Via Blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1-11, 2018.

[12] Floyd T., Grieco M., and Reid E., "Mining Hospital Data Breach Records: Cyber Threats to US Hospitals," *in Proceedings of IEEE Conference on Intelligence and Security Informatics*, Tucson, pp. 43-48, 2016.

[13] Fontaine C. and Galand F., "A Survey of Homomorphic Encryption for Nonspecialists," *EURASIP Journal on Information Security*, vol. 1, no. 013801, pp. 1-7, 2007.

[14] Jiang W., Xu H., Dong H., Jin H., and Liao X., "An Improved Security Framework for Web Service-Based Resources," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 24, no. 3, pp. 774-79, 2016.

[15] Jaidi F., Ayachi F., and Bouhoula A., "Advanced Analysis of the Integrity of Access Control Policies: The Specific Case of Databases," *The International Arab Journal of Information Technology*, vol. 17, no. 5, pp. 808-815, 2020.

[16] Kanwal T., Anjum A., and Khan A., "Privacy Preservation in E-Health Cloud: Taxonomy, Privacy Requirements, Feasibility Analysis, and Opportunities," *Cluster Computing*, vol. 24, no. 1, pp. 293-317, 2021.

[17] Kenthapadi K., Mironov I., Thakurta A., "Privacy-preserving Data Mining in Industry," *in Proceedings of the 12th ACM International Conference on Web Search and Data Mining*, New York, pp. 840-841, 2019.

[18] Kenthapadi K., Mishra N., and Nissim K., "Simulatable Auditing," *in Proceedings of the 24th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, Baltimore-Maryland, pp. 118-127, 2005.

[19] Khozaimi A., Putro S., and Yaqin A., "Improve The Performance and Security of Medical Records using Fingerprint and Advance Encryption Standart," *in Proceedings of*

International Conference on Health Informatics, Medical, Biological Engineering, and Pharmaceutical, Jakarta, pp. 285-290, 2020.

[20] Kleinberg J., Kumar R., Raghavan P., Rajagopalan S., and Tomkins A., "The Web as a Graph: Measurements, Models, and Methods," *in Proceedings of International Computing and Combinatorics Conference*, Tokyo, pp. 1-17, 1999.

[21] Langenberg B., Pham H., and Steinwandt R., "Reducing The Cost of Implementing The Advanced Encryption Standard as A Quantum Circuit," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1-12, 2020.

[22] Li J., Yu Q., Zhang Y., and Shen J., "Key-Policy Attribute-Based Encryption Against Continual Auxiliary Input Leakage," *Information Sciences*, vol. 470, pp.175-188, 2019.

[23] Liu L., Lai J., Deng R., and Li Y., "Ciphertext-Policy Attribute-Based Encryption with Partially Hidden Access Structure and its Application to Privacy-Preserving Electronic Medical Record System in Cloud Environment," *Security and Communication Networks*, vol. 9, no. 18, pp. 4897-4913, 2016.

[24] Luo W. and Ma W., "Secure And Efficient Proxy Re-Encryption Scheme Based on Key-Homomorphic Constrained Prfs in Cloud Computing," *Cluster Computing*, vol. 22, no. 2, pp. 541-551, 2019.

[25] Mahanta H. and Khan K., "Securing RSA Against Power Analysis Attacks Through Non-Uniform Exponent Partitioning with Randomization," *IET Information Security*, vol. 12, no. 1, pp. 25-33, 2018.

[26] Marwan M., AlShahwan F., Sifou F., Ali K., and Ouahmane H., "Improving the Security of Cloud-based Medical Image Storage," *Engineering Letters*, vol. 27, no. 1, pp. 175-193, 2019.

[27] McDermott D., Kamerer J., and Birk A., "Electronic Health Records: A Literature Review of Cyber Threats and Security Measures," *International Journal of Cyber Research and Education*, vol. 1, no. 2, pp. 42-49, 2019.

[28] Mukti G. and Setiawan H., "Designing and Building Secure Electronic Medical Record Application by Applying AES-256 and RSA Digital Signature," *IOP Conference Series: Materials Science and Engineering*, vol. 852, no. 1, pp. 0121482019, 2019.

[29] Osamor V. and Edosomwan I., "Employing Scrambled Alpha-Numeric Randomization and RSA Algorithm to Ensure Enhanced Encryption in Electronic Medical Records," *Informatics in Medicine Unlocked*, vol. 25, pp. 100672, 2021.

[30] Ostrovsky R., Sahai A., and Waters B., "Attribute-Based Encryption with Non-Monotonic Access Structures," *in Proceedings of the 14th ACM Conference on Computer and Communications Security*, Virginia, pp. 195-203, 2007.

[31] Prathap R., Mohanasundaram R., and Kumar P., "Design of EHR in Cloud with Security," *in Proceedings of Smart Intelligent Computing and Applications*, Singapore, pp. 419-425, 2019.

[32] Pugazhenthi A. and Chitra D., "Secured and Memory Overhead Controlled Data Authentication Mechanism in Cloud Computing," *Cluster Computing*, vol. 22, no. 6, pp. 13559-13567, 2019.

[33] Qian H., Li J., Zhang Y., and Han J., "Privacy-Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487-497, 2015.

[34] Rezaeibagha F. and Mu Y., "Distributed Clinical Data Sharing Via Dynamic Access-Control Policy Transformation," *International Journal of Medical Informatics*, vol. 89, pp. 25-31, 2016.

[35] Samkari H. and Gutub A., "Protecting Medical Records against Cybercrimes within Hajj Period by 3-layer Security," *Recent Trends in Information Technology and its Application*, vol. 2, no. 3, pp. 1-21, 2018.

[36] Sánchez Y., Demurjian S., Baihan M., "A Service-Based RBAC and MAC Approach Incorporated into the FHIR Standard," *Digital Communications and Networks*, vol. 5, no. 4, pp. 214-225, 2019.

[37] Shaqrah A. and Noor T., *Data Analytics in Medicine: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2020.

[38] Sharma B., Sekharan C., and Zuo F., "Merkle-Tree Based Approach for Ensuring Integrity of Electronic Medical Records," *in Proceedings of 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference*, New York, pp. 983-987, 2018.

[39] Sharma K., Agrawal A., Pandey D., Khan R., and Dinkar S., "RSA Based Encryption Approach for Preserving Confidentiality of Big Data," *Journal of King Saud University-Computer and Information Sciences*, 2019.

[40] Shen N., Bernier T., Sequeira L., Strauss J., Silver M., Carter-Langford A., and Wiljer D., "Understanding the Patient Privacy Perspective on Health Information Exchange: A Systematic Review," *International Journal of Medical Informatics*, vol. 125, pp. 1-12, 2019.

[41] Singh N., Jangra A., Elamvazuthi I., Kashyap K., "Healthcare Data Privacy Measures To Cure and Care Cloud Uncertainties," *in Proceedings of International Conference on Signal Processing, Computing and Control*, Solan, pp. 402-407, 2017.

[42] Song D., Wagner D., and Perrig A., "Practical Techniques for Searches on Encrypted Data," *in Proceedings of IEEE Symposium on Security and Privacy*, Berkeley, pp. 44-55, 2000.
[43] Soni K. and Kumar S., "Comparison of RBAC and ABAC Security Models for Private Cloud," *in Proceedings of International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, Faridabad, pp. 584-587, 2019.
[44] Tuncer T. and Avcı E., "Data Hiding Application with Gokturk Alphabet Based Visual Cryptography Method," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 31, no. 3, pp. 781-789, 2016.
[45] Wang Q., Peng L., Xiong H., Sun J., and Qin Z., "Ciphertext-Policy Attribute-Based Encryption with Delegated Equality Test in Cloud Computing," *IEEE Access*, vol. 6, pp. 760-771, 2017.
[46] Woźniak M., Graña M., and Corchado E., "A Survey of Multiple Classifier Systems as Hybrid Systems," *Information Fusion*, vol. 16, pp. 3-17, 2014.
[47] Yang J., Li J., and Niu Y., "A Hybrid Solution For Privacy Preserving Medical Data Sharing in The Cloud Environment," *Future Generation Computer Systems*, vol. 43, pp. 74-86, 2015.
[48] Yesmin T. and Carter M., "Valuation Framework for Automatic Privacy Auditing Tools for Hospital Data Breach Detections and an Application Case," *International Journal of Medical Informatics*, pp. 104123, 2020.
[49] Yılmaz N. and Tarhan A., "A Two-Dimensional Method for Evaluating Maintainability and Reliability of Open Source Software," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 34, no. 4, pp. 1807-1830, 2019.
[50] Zheng L., Zhang Y., Zhang R., Chen J., Cui M., and Song C., "An Improved Authentication Protocol in Telemedicine System," *in Proceedings of International Conference on Algorithms and Architectures for Parallel Processing*, Guangzhou, pp. 177-184, 2018.

Ömer Kasim (Orcid ID: 0000-0003-4021-5412) is a member of faculty in the Department of Electric and Electronics Engineering at Kutahya Dumlupinar University as an associate professor. He holds a PhD degree from Marmara University institute of science. His research focus is the artificial intelligence, biomedical engineering and cyber security. He has been publishing regarding this topic for the past decade.